



# **NAVAL POSTGRADUATE SCHOOL**

**MONTEREY, CALIFORNIA**

## **THESIS**

**DEVELOPMENT OF FUTURE COURSE CONTENT  
REQUIREMENTS SUPPORTING THE DEPARTMENT OF  
DEFENSE'S INTERNET PROTOCOL VERSION 6  
TRANSITION AND IMPLEMENTATION**

by

James T. Kay

June 2006

Thesis Advisor:

Co-Advisor:

Second Reader:

Geoffrey Xie

John Gibson

Kristen Tsois

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
<b>1. AGENCY USE ONLY (Leave blank)</b>		<b>2. REPORT DATE</b> June 2006	<b>3. REPORT TYPE AND DATES COVERED</b> Master's Thesis	
<b>4. TITLE AND SUBTITLE:</b> Development of Future Course Content Requirements Supporting the Department of Defense's Internet Protocol Version 6 Transition and Implementation			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> James T. Kay				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release; distribution is unlimited			<b>12b. DISTRIBUTION CODE</b>	
<b>13. ABSTRACT (maximum 200 words)</b> This thesis will focus on academia, specifically the Naval Postgraduate School, and its requirement to implement an education program that allows facilitators to properly inform future students on the gradual implementation of Internet Protocol version 6 (IPv6) technology while phasing out Internet Protocol version 4 (IPv4) from the current curriculum as the transition to IPv6 progresses. The DoD's current goal is to complete the transition of all DoD networks from IPv4 to IPv6 by fiscal year 2008. With this deadline quickly approaching, it is imperative that a plan to educate military and DoD personnel be implemented in the very near future. It is my goal to research and suggest a program that facilitators can use that will show the similarities, changes, advantages, and challenges that exist for the transition.				
<b>14. SUBJECT TERMS</b> IPv6 Transition, IPv6 Education, NPS Curriculum, Next Generation Network, IPv4 to IPv6,			<b>15. NUMBER OF PAGES</b> 69	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UL	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)  
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**DEVELOPMENT OF FUTURE COURSE CONTENT REQUIREMENTS  
SUPPORTING THE DEPARTMENT OF DEFENSE'S INTERNET PROTOCOL  
VERSION 6 TRANSITION AND IMPLEMENTATION**

James T. Kay  
Captain, United States Marine Corps  
B.S., Auburn University, 1998

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL  
June 2006**

Author: James T. Kay

Approved by: Geoffrey Xie  
Thesis Advisor

John Gibson  
Co-Advisor

Kristen Tsolis  
Second Reader

Dan C. Boger  
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

This thesis will focus on academia, specifically the Naval Postgraduate School, and its requirement to implement an education program that allows facilitators to properly inform future students on the gradual implementation of Internet Protocol version 6 (IPv6) technology while phasing out Internet Protocol version 4 (IPv4) from the current curriculum as the transition to IPv6 progresses.

Currently, the largest Internet Protocol (IP) network in the world is run by the Department of Defense (DoD). Internet Protocol provides the critical functionality that enables stable, reliable communications, and survivability of information between computers across various network types, including local area networks and wide area networks. Used for almost 30 years, IPv4 is implemented on a wide range of computing and networking platforms. The emerging replacement for the long standing IPv4 is the new Internet protocol which is IPv6. The current plan calls for IPv6 to coexist with IPv4 during a transition period; but it will eventually replace IPv4 in most networks.

The DoD's current goal is to complete the transition of all DoD networks from IPv4 to IPv6 by fiscal year 2008. With this deadline quickly approaching, it is imperative that a plan to educate military and DoD personnel be implemented in the very near future. It is my goal to research and suggest an education program that facilitators can use and will show the similarities, changes, advantages, and challenges that exist for the transition. At present, the Defense Information Systems Agency has organized a working group and assigned different commands to focus on the transition to IPv6.

THIS PAGE INTENTIONALLY LEFT BLANK

## TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>A.</b>	<b>BACKGROUND .....</b>	<b>1</b>
<b>B.</b>	<b>OBJECTIVES .....</b>	<b>1</b>
<b>C.</b>	<b>QUESTIONS FOR RESEARCH.....</b>	<b>2</b>
<b>D.</b>	<b>SCOPE .....</b>	<b>2</b>
<b>E.</b>	<b>METHODOLOGY .....</b>	<b>3</b>
<b>F.</b>	<b>THESIS ORGANIZATION.....</b>	<b>3</b>
<b>II.</b>	<b>COMPARISON BETWEEN IPV4 AND IPV6 .....</b>	<b>5</b>
<b>A.</b>	<b>STRENGTHS, WEAKNESSES, AND DIFFERENCES BETWEEN INTERNET PROTOCOLS.....</b>	<b>5</b>
1.	Larger Address Space.....	5
2.	Simplified Header Structures .....	6
3.	Auto-configuration and Neighbor Discovery .....	7
4.	Better Support for Quality of Service (QoS) .....	8
5.	Multicast Capability Supporting Enhanced Mobility Features .....	9
6.	Integrated Internet Protocol Security .....	9
<b>B.</b>	<b>PROPOSED TRANSITION IMPLEMENTATION METHODS AND COVERT CHANNELS .....</b>	<b>11</b>
1.	Dual IP Stack.....	11
2.	Tunnels.....	12
a.	<i>Configured Tunnels .....</i>	<i>12</i>
b.	<i>Automatic Tunnels and Tunnel Brokers.....</i>	<i>12</i>
3.	Translation.....	12
4.	Central Backbone Theory .....	13
<b>C.</b>	<b>RISKS AND SECURITY ISSUES .....</b>	<b>13</b>
1.	Authorization for Automatically Assigned Addresses and Configurations.....	13
2.	Protection of IP Packets .....	14
3.	Host Protection from Scanning and Attacks.....	15
<b>III.</b>	<b>EDUCATION IMPLEMENTATION INTO NAVAL POSTGRADUATE SCHOOL CURRICULUM .....</b>	<b>19</b>
<b>A.</b>	<b>OFFICE OF MANAGEMENT AND BUDGET TIMELINE REQUIREMENT.....</b>	<b>19</b>
1.	Initial Directives.....	19
2.	OMB Timeline Guideline Memorandum M-05-22 .....	20
a.	<i>November 15, 2005.....</i>	<i>20</i>
b.	<i>February 2006.....</i>	<i>20</i>
c.	<i>June 30, 2006 .....</i>	<i>20</i>
d.	<i>June 30, 2008 .....</i>	<i>20</i>

B.	RECOMMENDED IPV6 INCLUSION FOR SELECTED COURSES AT THE NAVAL POSTGRADUATE SCHOOL.....	22
1.	Course IS3502 – Fundamentals of Networks: LAN/WAN.....	23
2.	Course IS4188 – Collaborative Technologies.....	24
3.	Course IS4505 – Wireless Networking.....	24
4.	Course IS4926 – Telecommunications and Network Operating Centers .....	25
5.	Course CS3502 – Computer Communications and Networks.....	26
6.	CS3505 – The Internet and the Information Highway.....	26
7.	Course CS3600 – Information Assurance: Introduction to Computer Security.....	27
8.	Course CS3660 – Critical Infrastructure Protection.....	27
9.	Course CS3670 – Information Assurance: Secure Management of Systems .....	28
10.	Course CS3690 – Network Security .....	28
11.	Course CS4138 – Mobile and Wireless Security .....	29
12.	Course CS4550 – Computer Networks II .....	29
13.	Course CS4552 – Network Design & Programming .....	30
14.	Course CS4675 – Intrusion Detection and Response .....	30
15.	Course CS4678 – Advanced Vulnerability Assessment.....	31
C.	IPV6 EDUCATION OUTSIDE NAVAL POSTGRADUATE SCHOOL. ....	31
1.	Universities .....	32
2.	Consulting Firms and Training Companies.....	33
a.	<i>Native6 Incorporated</i> .....	33
b.	<i>Cisco Systems</i> .....	33
c.	<i>TONEX</i> .....	34
3.	Other Education Opportunities.....	34
a.	<i>Defense Information Systems Agency</i> .....	35
b.	<i>The Internet Engineering Task Force (IETF)</i> .....	35
D.	CHAPTER CONCLUSION.....	35
IV.	THE NAVAL POSTGRADUATE SCHOOL’S PROGRESS TOWARDS IPV6 TRANSITION .....	37
A.	BACKGROUND .....	37
B.	PROGRESS TO DATE .....	39
1.	Monterey Peninsula IPv6 Working Group Consortium .....	39
2.	The Plan for Naval Postgraduate School.....	39
C.	FUTURE PLANS.....	40
D.	OTHER CHALLENGES AND DECISIONS.....	40
1.	IPv6 Training .....	40
2.	Vendor Selection .....	41
V.	RECOMMENDATIONS AND CONCLUSION.....	43
A.	IMPORTANCE OF IPV6 EDUCATION IN THE CURRICULUM.....	43
B.	THE BIGGEST CHALLENGES TO LEARNING .....	44
C.	FURTHER RESEARCH TOPICS.....	45

<b>BIBLIOGRAPHY .....</b>	<b>47</b>
<b>INITIAL DISTRIBUTION LIST .....</b>	<b>49</b>

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF FIGURES

Figure 1.	IPv4 and IPv6 Comparison. (GAO, 2005).....	6
Figure 2.	IPv4 and IPv6 Header Differences. (GAO, 2005) .....	7
Figure 3.	Example of Dual IP Stack (GAO, 2005) .....	11
Figure 4.	Example of Tunneling (GAO, 2005) .....	12
Figure 5.	IPv6 Deadlines Established by OMB (Geesey, 2006).....	21
Figure 6.	DoD's Schedule for IPv6 Transition (GAO, 2005) .....	22
Figure 7.	Basic Diagram of NPS's Current Network Infrastructure .....	38
Figure 8.	Basic Diagram of NPS's Future Network Infrastructure with CalNET HPR Connection .....	38

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

Table 1.	Major Differences Between IPv4 and IPv6 (Davies, 2003). .....	10
Table 2.	Native6's Education Offerings (Native6 Website) .....	33

THIS PAGE INTENTIONALLY LEFT BLANK

## ACRONYMS AND ABBREVIATIONS

AH	Authentication Header
CalREN DC	California Research and Education Network Digital California
CalREN HPR	California Research and Education Network High Performance Research
CENIC	Corporation for Education Networking in California
COTS	Commercial-Off-The-Shelf
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DISR	DOD Information Technology Standards Registry
DLI	Defense Language School
DMDC	Defense Manpower Data Center
DREN	Defense Research and Engineering Network
ESP	Encapsulating Security Payload
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISATAP	Automatic Tunnel Addressing Protocol
ISP	Internet Service Provider
JITC	Joint Interoperability Test Command
MIPv6	Mobile Internet Protocol 6
NAT	Network Address Translator
NAv6TF	North American IPv6 Task Force
NMCI	Navy Marine Corps Intranet
NPS	Naval Postgraduate School
NRL	Naval Research Laboratory
OMB	Office of Management and Budget

PERSEREC	Defense Personnel Security Research Center
QoS	Quality of Service
RFC	Request for Comment
SEND	Secure Neighbor Discovery
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

## **ACKNOWLEDGMENTS**

I would like to thank Geoffrey Xie for his guidance and recommendations for pursuing the subject of Internet Protocol version 6. His ideas and suggestions helped steer the way for this thesis to be possible. I appreciate his allowance to participate in the IPv6 working group here at NPS in the Department of Computer Science which provided a large insight into the subject of IPv6 and aided in my push for a thesis completion.

My sincere thanks and gratitude go to my thesis co-advisor Mr. John Gibson for all of his hard work, guidance, insights, patience and tremendous support during the writing of my thesis. His assistance and support were instrumental to my successful completion.

As my second reader I would like to thank Kristen Tsolis for her time, effort, and suggestions that helped make this thesis a success. I also would like to thank her for the incredible instruction during IS3502 which was instrumental in laying the foundation for this thesis and understanding topics encountered while writing this paper.

I would also like to thank Bill Hogan for all the information, conversation, and knowledge you bestowed upon me concerning the changes to NPS's network system. You were of tremendous help and very patient.

My thanks also go to Dr. Christine Cermak, Lonna Sherwin, Terri Brutzman and Mike Yee for all of their time and efforts in corresponding to emails and personal interviews concerning IPv6 and NPS's network system. Your information has been incredibly enlightening and critical to my thesis completion.

To my wonderful and supporting family, thank you Brandon, Blake, Johnathon, Alexys and little Ayden for being the most patient and understanding kids a father can ask for. Your energies and thoughtful concerns about my thesis completion and school work are truly felt. Now I can truly focus on watching you grow up. To my beautiful and wonderful wife Samantha, thank you for being so supportive, encouraging, patient and understanding during this tour of duty and throughout my Marine Corps career. I

fully appreciate the huge sacrifices you have made during this time while trying to accomplish your own dreams in education. I only hope I can provide the same focus and attention you provided to me as you finish your own dissertation. I look forward to the rest of our lives together.

# **I. INTRODUCTION**

## **A. BACKGROUND**

Currently, the largest Internet Protocol (IP) network in the world is run by the Department of Defense (DoD). Internet Protocol provides the critical functionality that enables stable, reliable communications, and survivability of information between computers across various network types, including local area networks and wide area networks. Used for almost 30 years, Internet Protocol version 4 (IPv4) is implemented on a wide range of computing and networking platforms. The emerging replacement for the long standing IPv4 is Internet Protocol version 6 (IPv6). The DoD's current plan calls for IPv6 to coexist with IPv4 during a transition period; but it will eventually replace IPv4 in most networks.

The DoD's current goal is to complete the transition of all DoD networks from IPv4 to IPv6 by fiscal year 2008 (GAO, 2005). With this deadline quickly approaching, it is imperative that a plan to educate military and DoD personnel be implemented in the very near future. It is my goal to research and suggest an education program that facilitators can use that will show the similarities, changes, advantages, and challenges that exist for the transition. At present, the Defense Information Systems Agency has organized a working group and assigned different commands to focus on the transition to IPv6

## **B. OBJECTIVES**

The primary objective of this research is to identify and understand the changes that will be created by the transition from IPv4 to IPv6 and apply this understanding to the networking curricula already in place at the Naval Postgraduate School (NPS) in efforts to prepare future graduates for upcoming job assignments within the government. A gradual implementation of critical IPv6 topics must be incorporated into all curriculum programs involving the education of students at NPS while phasing out old and outdated information that will no longer apply once IPv6 becomes fully implemented throughout the DoD in the next couple of years. This will give graduates of NPS the foundation to understand and apply the knowledge learned at NPS on possible job assignments in the military involving IPv6.

A second objective is to examine NPS's own progress towards transitioning its campus network system to an IPv6 capable system. This will open the possibly for future thesis research by students at NPS while also helping to prepare NPS for the upcoming changes.

The last objective is to research a practical way to implement a curriculum that can be used DoD wide in efforts to educate military and federal employees and prepare them for changes that will occur by the transition to IPv6.

### **C. QUESTIONS FOR RESEARCH**

1. What are the key elements of IPv6, mainly strengths and weaknesses, that are the drivers for the DoD decision to transition to it?
2. What are the similarities and changes between IPv4 and IPv6?
3. What are the risks and security issues involved with the transition to IPv6 and how will it affect implementation in the current academic curriculum?
4. What barriers exist to prevent proper education on IPv6?
5. What is the coverage of IPv6 in the current Naval Postgraduate School curricula?
6. What resources are available outside Naval Postgraduate School for educating military and DOD personnel on IPv6?
7. How should IPv6 be implemented in an academic environment such as the Naval Postgraduate School?
8. How prepared is the Naval Postgraduate School's own network for IPv6?

### **D. SCOPE**

This thesis will focus on exploring the differences, changes, similarities, strengths, weakness, security, and risks of transitioning to IPv6 from IPv4. Based on this research information, the question of what changes should be implemented in the specific NPS curricula to address the transition will be answered and developed. This will help ensure that NPS has a faculty fully prepared to teach these changes as the transition to IPv6 approaches. Additionally, it will help ensure that NPS's own networks are fully prepared to embrace the changes. Continuation of this thesis can expand the scope to cover military service technical training schools and other graduate and educational institutions that support DoD agencies and military personnel.

## **E. METHODOLOGY**

This thesis will be based on research, qualitative study methods that include an examination of the syllabi of networking courses offered at NPS, interviews with select faculty members, and methods already being explored, used, and proven by the Defense Information Systems Agency. In addition, agencies outside the government and in other countries will be examined and researched. The results of interviews and research will then be used to successfully implement a curriculum to properly educate those personnel exposed to the curriculum. Some information gathered will be from the results of experiments being conducted by other students working simultaneously on different aspects of IPv6.

## **F. THESIS ORGANIZATION.**

Chapter II covers the majority of information that concerns the transition to IPv6. Specifically, it focuses on the strengths and weaknesses; similarities and differences; and the security and risks of the transition that are pertinent to educating students on IPv6.

Chapter III identifies current curriculum instruction topics and creates a time table for phasing in important and pertinent IPv6 material while slowly moving away from IPv4 topics that will no longer be of importance or apply once the transition is complete. Additionally, focus turns to organizations outside of NPS to examine feasible means for educating service branch members as well as federal employees of the government that may be responsible for IPv6 implementation or routine interactions with IPv6.

Chapter IV focuses on NPS's current progress towards the IPv6 transition and outlines future plans, foreseeable problems and possible timelines for milestone achievements for the successful transition to IPv6.

Chapter V summarizes the major findings, suggestions, and findings as well as the problems encountered during the thesis research. It also makes recommendations for future thesis research.

THIS PAGE INTENTIONALLY LEFT BLANK

## **II. COMPARISON BETWEEN IPV4 AND IPV6**

### **A. STRENGTHS, WEAKNESSES, AND DIFFERENCES BETWEEN INTERNET PROTOCOLS**

To implement a plan to introduce IPv6 topics into the NPS curriculum, it is important to identify major changes that students and faculty must understand. There are many topics to consider when examining the transition to IPv6 and how it applies to the learning of students and educators. The predominant and most widely covered topics will be presented in this chapter. Other topics will become inherently important as IPv6 continues to develop and be implemented over the period of the transition. Like all new technologies, continuous development will create new challenges to the people that operate and monitor the new technologies and will create opportunities for someone on the other end trying to exploit or misuse that technology.

#### **1. Larger Address Space**

No one would have imagined that the Internet explosion would exhaust and make relatively scarce the number of public IP addresses available for allocation. IPv4 currently allows for 4,294,967,296 addresses using its 32-bit address space. Places like Europe and Asia were forced to look at IPv6 primarily because they were only given a small portion of the IP address allocation despite having a much larger population than the United States. Many organizations and businesses still using IPv4 have been forced to use Network Address Translators (NAT) to map a single public IP address into many private address spaces. These NATs create bottlenecks and reduce the performance of software applications (Davies, 2003).

To alleviate this issue, IPv6 introduces a 128-bit address, which equates to over  $3.4 \times 10^{38}$  possible combinations for IP addresses, as shown in Figure 1. This will allow for the expansion of IP addresses to peripherals other than computers such as PDA's, watches, and possibly even household appliances in the future. Basically, there would be  $6.65 \times 10^{23}$  addresses available per every square meter on the Earth's surface (Davies, 2003).

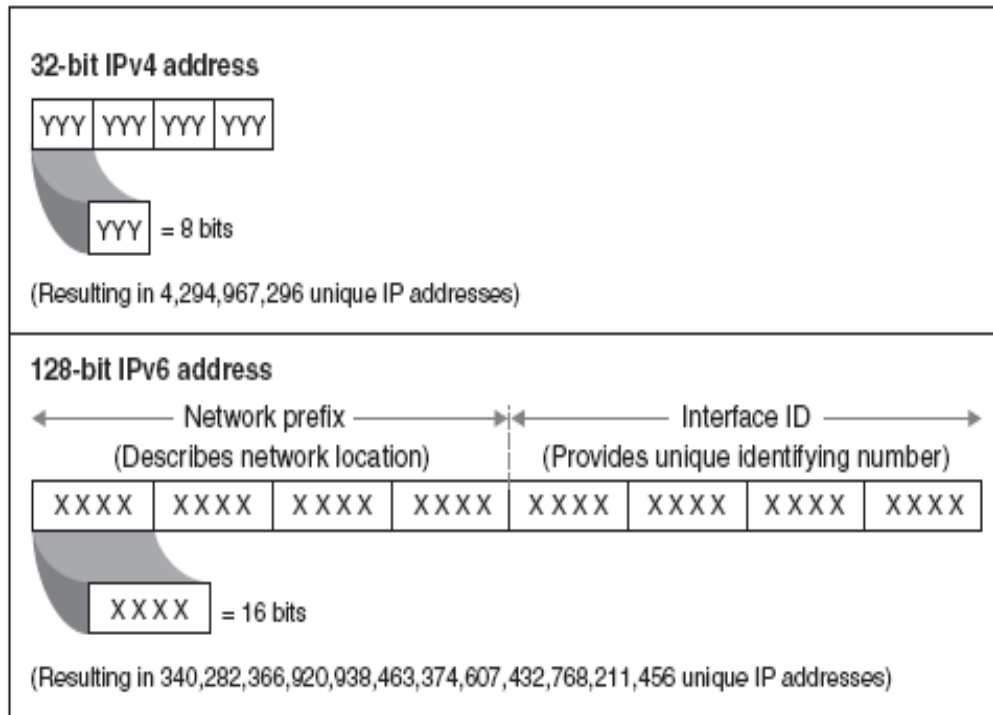


Figure 1. IPv4 and IPv6 Comparison. (GAO, 2005)

## 2. Simplified Header Structures

Simplified header structures provide flexibility and functionality in two ways. First, the header size in IPv6 is fixed. This aids in speeding the routing of information. Secondly, the structure of the IPv6 header has been simplified despite having a larger address. IPv4 uses 14 header fields while IPv6 only uses eight. The difference is shown explicitly in Figure 2. This simplification allows for other features and extensions to be added later (GAO, 2005). Header overhead is minimized by moving nonessential and optional fields to extension headers that are placed after the IPv6 header.

A consequence of this change is that IPv6 is not a superset of IPv4 and is therefore not interoperable with it. This requires that hosts or routers be able to differentiate between the two IP versions and be able to recognize and process both versions unless a pure IPv6 backbone exists (Davies, 2003). For this reason, it is suggested that a tunneling method will most likely be utilized to implement IPv6 during the transition until a pure and complete IPv6 backbone is established within the DoD network.

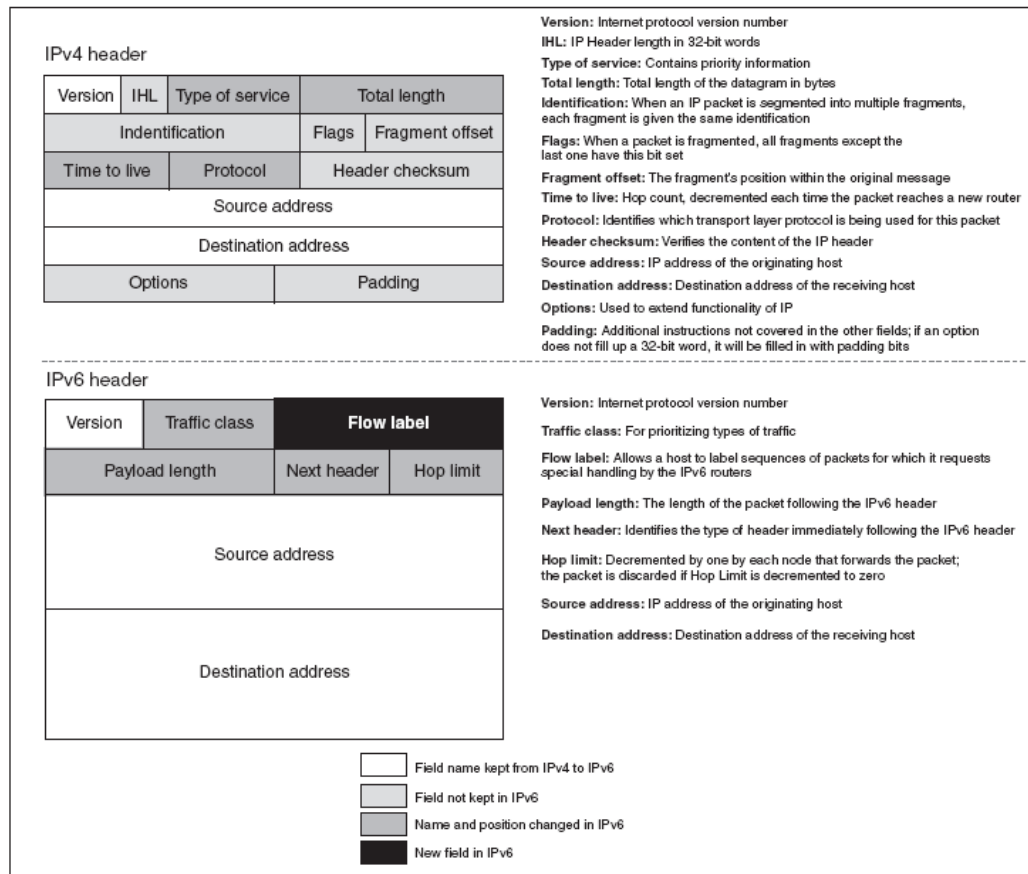


Figure 2. IPv4 and IPv6 Header Differences. (GAO, 2005)

A more efficient, hierarchical, and summarized routing infrastructure will be established due to the IPv6 global addresses. This will provide for smaller more simplified routing tables which currently plague IPv4 routing tables. Again, the end benefit is router performance improvement (GAO, 2005).

### 3. Auto-configuration and Neighbor Discovery

IPv6 allows for IP addresses and other network-related parameters to be configured automatically. This reduces the burden placed on administrators. Additionally, it allows for neighbor discovery. The auto-configuration supports both stateful and stateless address configuration.

With stateless address configurations, hosts on a link automatically configure themselves with IPv6 addresses for the link (called link-local addresses), addresses for IPv4 and IPv6 coexistence, and with addresses derived from prefixes advertised by local routers. Even in the absence of a router, hosts on the same link can automatically configure themselves with link-local addresses and communicate without manual configuration.

Link-local addresses are auto configured within one second of time and communication with neighboring nodes on the link is possible immediately (Davies, 2003).

Neighbor discovery enables routers and hosts to determine addresses of adjoining computers or routers. Combined with automatic configuration, support is available to allow deployment of many different devices such as PDA's, cell phone, and even household appliances, as already mentioned. IPv6 enabling devices can automatically assign themselves IP addresses and locate other devices with which to communicate (GAO).

This is a very important concept for future Naval Postgraduate students to understand should they become a network administrator in the future. Unfortunately, the ability for auto-configuration leaves networks open for attacks and abuse if not managed properly and will be covered in greater detail at the end of this chapter. Some operating systems currently allow for IPv6 auto-configuration. If this capability is intentionally or unintentionally activated without knowing the hazards, serious network vulnerabilities may be exploited. An attack may occur because an unauthorized router may reconfigure neighboring devices by assigning new routes or addresses. Anyone with the duties of interacting with such operating system capability should be aware of the hazards posed by inadvertently activating the auto-configuration mode.

#### **4. Better Support for Quality of Service (QoS)**

IPv6 headers will support real-time and priority traffic via a Traffic Class field. The Flow Label field in the IPv6 header allows routers to identify and provide special handling for packets belonging to a flow. The QoS is achieved despite Internet Protocol Security (IPSec) and Encapsulating Security Payload (ESP) because traffic is identified in the IPv6 header. At this time, there are details that have yet to be resolved. According to David Green and Bob Grillo, members of SRI International, QoS for IPv6 is no better than the current QoS provided by IPv4. The hype of IPv6 QoS is not making the grade for claims made concerning this topic. The main reason for this is due to the DoD lacking key guidance on the flow label that provides better QoS handling (2005).

Graduate students should be familiar with this concept and, due to lacking guidance, this topic should be closely followed and covered in the curriculum. Further thesis research is a strong possibility for students in the future.

## **5. Multicast Capability Supporting Enhanced Mobility Features**

Mobility is of great interest to the DoD due to our Global War on Terrorism and the military's constant deployment of communication systems to areas void of communication infrastructure. IPv6 makes the capabilities of a mobile network routine by the use of non-perishable global addresses and using network elements that remain in an always-on state. This means an improved version of Mobile IPv6 (MIPv6) which allows mobile nodes to connect in different areas without a disruption of communications. "The MIPv6 protocol, residing in the IPv6 protocol stack, allows the mobile node, home agent, and corresponding node to exchange 'care of' address information of the mobile node so that the two end nodes may update the routing information and communicate along the shortest path to each other, bypassing the home agent (Green, 2005)."

## **6. Integrated Internet Protocol Security**

A means to provide private communications over the Internet requires cryptographic services. The standard for providing this service in IPv4 is known as Internet Protocol Security or IPsec. This standard is optional for IPv4 and was developed as an afterthought for IPv4. IPv6 fully integrates IPsec per Request For Comment (RFC) 2460, which states that "full implementation" must include implementation of authentication headers (AH) and Encapsulating Security Payload (ESP) headers. This will allow easier use of IP Security for providing better data protection. IPsec in IPv6 consists of two header extensions. They are used together or separately to improve confidentiality and authentication of data being transmitted via the Internet. By using the authentication extension header, greater assurance is provided to the receiver as to who sent the data (GAO, 2005).

On the next page is a table that highlights the key differences between the two Internet Protocol versions. The table depicts more topics than will be chosen for implementation into the curriculum transition plan for the Naval Postgraduate School, but gives the reader a view of the major changes. As time progress, more and more of the

topics concerning IPv6 should be incorporated into the curriculum as they evolve and become mature. In addition, as more of the IPv4 topics are no longer applicable in the years to come, they should be dropped from future course work except in cases when it may be necessary to explain how something was accomplished back in the days of IPv4.

<b>IPv4</b>	<b>IPv6</b>
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
IPSec support is optional.	IPSec support is required.
No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is present within the IPv6 header using the Flow Label field.
Fragmentation is performed by the sending host and at routers, slowing router performance.	Fragmentation is performed only by the sending host.
Has no link-layer packet size requirements and must be able to reassemble a 576-byte packet.	Link layer must support a 1,280-byte packet and must be able to reassemble a 1,500-byte packet
Header includes a checksum.	Header does not include a checksum.
Header includes options.	All optional data is moved to IPv6 extension headers.
ARP uses broadcast ARP Request frames to resolve an IPv4 address to a link-layer address	ARP Request frames are replaced with multicast Neighbor Solicitation messages.
Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.	ICMPv4 Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.
Broadcast addresses are used to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.
Must be configured either manually or through DHCP for IPv4.	Does not require manual configuration or DHCP for IPv6.
Uses host address (A) resource records in the Domain Name System (DNS) to map host names to IPv4 addresses.	Uses AAAA records in the DNS to map host names to IPv6 addresses.
Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.INT DNS domains to map IPv6 addresses to host names.

Table 1. Major Differences Between IPv4 and IPv6 (Davies, 2003).

## B. PROPOSED TRANSITION IMPLEMENTATION METHODS AND COVERT CHANNELS

It is important for graduate students to understand that several ideas on how to migrate to IPv6 are being suggested by all organizations involved in the transition research. It must be realized that this is not a technology that can be turned on one day with the flip of switch, which is sometimes the case when a new system being implemented. Several of these ideas will now be covered. They are specifically important because they leave many questions unanswered and raise other questions concerning security and compatibility. Some of these questions concerning security will be covered at the end of this chapter.

To cope with the fundamental issues of this transition, the Internet Engineering Task Force (IETF) has designed two basic mechanisms.

### 1. Dual IP Stack

The preferred method by the GAO is a dual IP stack, also known as dual stack, which allows for both IPv4 and IPv6 support in hosts and routers. This enables IPv4 communications and traffic to exist when IPv6 is not supported by a network.

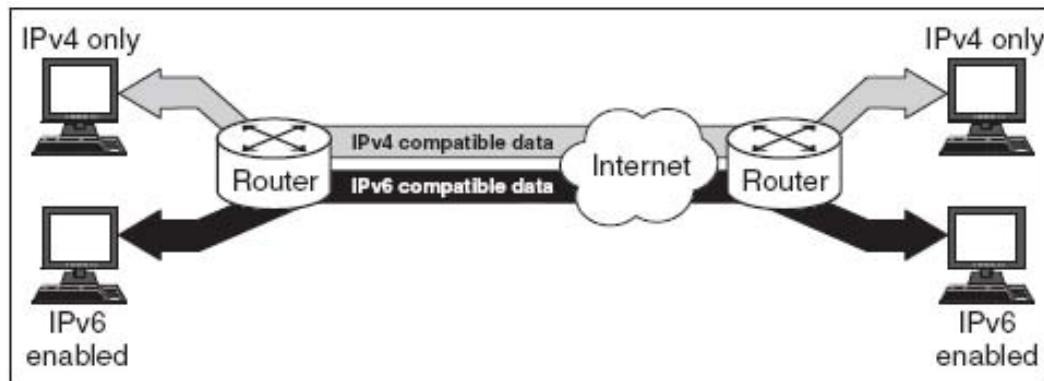


Figure 3. Example of Dual IP Stack (GAO, 2005)

This method is a widely used and executed technique. The exact methods the DoD intends to implement are still not clearly defined but must be done quickly if implementers, contractors, and developers are to implement the standards required in their products (Green, 2005).

## 2. Tunnels

Tunnels allow IPv6 networks to pass traffic and communicate with each other using an IPv4 backbone. The tunnels typically exist between two routers with the possibility of a user end station that will act as a tunnel end point. (GAO, 2005)

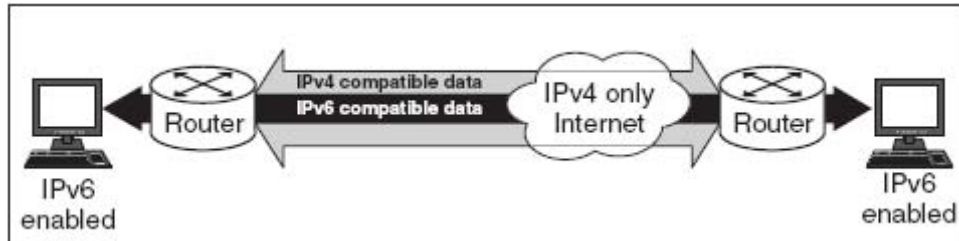


Figure 4. Example of Tunneling (GAO, 2005)

### a. Configured Tunnels

These are tunnels that are manually configured by a network administrator. They are easy to implement on a small scale or static network, but can be cumbersome for a larger, dynamic network.

### b. Automatic Tunnels and Tunnel Brokers

Automatic tunnels relieve network administrators from the labor intensive setup and configuration of tunnels in a large network. One way to accomplish this is by embedding the IPv4 address within the larger IPv6 address when encapsulating the original message. This method leaves a network vulnerable to malicious attacks because the tunnels allow hosts to make outside connections that could bypass security measures such as firewalls and intrusion detection systems (IDS).

A second method is by using a tunnel broker which maintains a translation table and IPv4 address that can be used when encapsulating the messages.

## 3. Translation

Translation allows for the two separate IPs to communicate with each other by translating IPv6 packets to IPv4 packets. This can provide a high level of interoperability because it allows new systems to deploy as IPv6 systems while IPv4 systems remain in place and are phased out. The drawback is a bottleneck can occur while the translation of packets is being executed (Green, 2005).

#### **4. Central Backbone Theory**

Although undocumented to the best of the author's knowledge, it has been suggested by J. D. Fulp, Lecturer at the Naval Postgraduate School, Monterey, CA, that

It would seem more efficacious to "grow" the IPv6 infrastructure from the inside-out, rather than the outside-in. The outside-in approach would necessitate end users and distribution layer infrastructure (routers) at the edge converting over to an addressing scheme that may or may not be supported by the upstream (internal to edge) routing and switching infrastructure. This effectively places the risk of adopting an insufficiently supported addressing scheme on the door step of the end user, and thus frustrates adoption and acceptance of the new scheme. The inside-out approach would start with a notional single IPv6-capable router in the "core". This single router would go unnoticed. The next step would be to add IPv6-capable routers one "hop" from the first single IPv6 router. IPv6 would be spoken between these routers. All routers and users more distal (toward the edge) from these co-rerouters would continue to run IPv4, and simply have their v4 traffic encapsulated inside of v6 headers when traversing the growing IPv6 core. This accretion process would continue until the v6 technology reached the edge. End users/systems could then continue to use v4 indefinitely, or transition to v6, knowing that either addressing scheme was supported. This dual-support infrastructure would seem easily supported if a simple v4-v6 conversion is used. That conversion would simply recognize any 32 bit IP address as v4, and convert it to v6 by pre-pending 96 zeroes; subsequently treating the resulting 128 bit address as a v4 backwards compatible v6 address. Should any such converted address reach a router that needs to route the packet forward to a v4 network, it would simply have the 96 pre-pended zeroes removed and the conversion back to IPv4 would be complete.

#### **C. RISKS AND SECURITY ISSUES**

With the upcoming IPv6 transition, there are certain potential risks and security issues that must be considered. They are important for graduate students to understand as they may accept the responsibilities as IT personnel at their next duty station and be faced with these challenges as this transition progresses. Microsoft Corporation provides some of the following guidelines and best practices.

##### **1. Authorization for Automatically Assigned Addresses and Configurations**

After gaining access to the network, any computer can obtain a valid IPv6 address configuration and begin communicating on the network. IPv6 hosts can use the following methods to obtain an IP address configuration:

- An exchange of Router Solicitation and Router Advertisement messages, as defined in RFC 2461. For Neighbor Discovery-based IPv6 configuration, Secure Neighbor Discovery (SEND) (described in RFC 3971) can provide protection for Router Solicitation and Router Advertisement messages. SEND can also be used to provide protection for Neighbor Solicitation and Neighbor Advertisement message exchanges for address resolution or neighbor unreachable detection, providing protection against Neighbor Discovery-based denial of service (DoS) attacks by nodes with statically configured IPv6 addresses. In contrast, there is no mitigation against Address Resolution Protocol (ARP) DoS attacks for IPv4.
- Dynamic Host Configuration Protocol for IPv6 (DHCPv6) defined in RFC 3315. RFC 3118 defines a method to provide authentication for DHCP message exchanges for IPv6 or IPv4 DHCP-based configuration.

IPv6 nodes will configure additional routes and addresses based on received Router Advertisement messages. Malicious nodes can configure local hosts with improper addresses and routes which may disrupt IPv6-based network connectivity.

Microsoft recommends running IEEE 802.1X authentication in order to authenticate all computers that are connecting to a network with wired or wireless connections. With IEEE 802.1X-based authentication at the link layer, computers cannot send any network traffic until they have authenticated themselves to a switch or wireless access point. Only after a successful IEEE 802.1X authentication can an IPv6-based computer use address auto-configuration protocols such as Neighbor Discovery or DHCPv6 to obtain an automatically assigned IPv6 address configuration.

## **2. Protection of IP Packets**

To help protect IP packets from tampering or data modification and interpretation or passive capturing by intermediate or neighboring nodes, IP packets can be protected with IPsec. As mentioned, IPsec uses cryptographic security services to provide tampering protection, spoofing protection, and optional encryption for IP packets.

To aid in the transition from IPv4 to IPv6, IPv6 transition technologies such as Intrasite Automatic Tunnel Addressing Protocol (ISATAP) and Teredo provide IPv6 connectivity between IPv6/IPv4 hosts that are separated by an IPv4 infrastructure through tunneling. Teredo is an IPv6 transition technology that provides address assignment and host-to-host automatic tunneling for unicast IPv6 traffic when IPv6/IPv4 hosts are located behind one or multiple IPv4 network address translators (NATs). To traverse IPv4

NATs, IPv6 packets are sent as IPv4-based User Datagram Protocol (UDP) messages.

Tunneled IPv6 traffic can be encapsulated in the following ways:

- Using an IPv4 header. ISATAP traffic is IPv6 traffic tunneled using an IPv4 header that has the IP Protocol field set to 41. To protect ISATAP traffic, configure IPsec for IPv4 policy settings to protect all traffic with the IP protocol set to 41.
- Using an IPv4 header and a UDP header. Teredo traffic is IPv6 traffic tunneled using an IPv4 header and UDP port 3544. To protect Teredo traffic, configure IPsec for IPv4 policy settings to protect all traffic with the source or destination UDP port set to 3544.

### **3. Host Protection from Scanning and Attacks**

Hosts can be scanned or attacked by malicious software (malware, such as viruses/worms) or users, even when connected to a private network. During a scan, an attacker attempts to determine the IP address of a host (an address scan) and the set of TCP and UDP ports being listened to by the host (a port scan). The attacker then attempts to access the services and resources of the host or otherwise compromise its security.

With IPv6, the scanning of a subnet for valid unicast IPv6 addresses is made much more difficult by the large number of possible addresses. On an IPv6 subnet, IPv6 addresses use 64 bits for the interface ID portion of the address. Therefore, an attacker must scan up to  $2^{64}$  possible addresses. In contrast, on an IPv4 subnet, an attacker must typically scan less than  $2^{10}$  possible IPv4 addresses.

To prevent a port scan, hosts should use a host-based stateful firewall. Host-based stateful firewalls, by default, silently discard all incoming traffic that does not correspond to either traffic sent in response to a request of the computer (solicited traffic) or traffic that has been specified as allowed (excepted traffic). Note that a host-based stateful firewall will not prevent an attacker from determining open ports on a host if those ports are being used for active communication or the ports correspond to a service being offered by the host. For example, you must configure the host-based firewall on a Web server host with an exception (allowance) for Hypertext Transfer Protocol (HTTP) traffic. Therefore, an attacker will be able to determine that the host is listening on TCP port 80, even though the host-based firewall is enabled.

Microsoft recommends using firewalls or another host-based stateful firewall that supports IPv6 traffic. Centrally configure the firewall for exceptions and other behavior through Computer Configuration Group Policy in an Active Directory environment.

#### **4 Control of What Traffic is Exchanged with the Internet**

To prevent unwanted traffic from the Internet, organizations typically deploy edge firewalls, proxies, and intrusion detection systems (IDSs). These security devices attempt to ensure that an attacker's traffic from the Internet cannot penetrate to the private network, such as when a host on the private network is compromised by malware and becomes reachable by malicious users on the Internet. Many of these security devices are not currently IPv6 capable and pose additional security risks for IPv6 traffic. As an example, an edge firewall or proxy device that is not aware of IPv6 or IPv6 tunneled traffic could pass that traffic to and from the Internet, creating a conduit for attacks from the Internet. The following behaviors attempt to mitigate this threat:

- To exchange tunneled packets with hosts on the IPv4 Internet, the edge device must in front of outbound IPv4-based UDP traffic or IPv4 protocol 41 packets to the Internet. If not, the traffic for current IPv6 tunneling mechanisms (such as ISATAP or Teredo) will not be able to traverse IPv4-edge firewalls to the Internet. Most modern IPv4-based firewall products for large organizations drop all outbound IPv4-based UDP traffic and IPv4 protocol 41 packets by default.
- The application or service that is being attacked must be IPv6-capable. Many network applications and services are not IPv6-capable and only work over IPv4.

As another example, an IDS that has been configured to detect the traffic associated with common attacks and malicious behavior for IPv4 might not be able to detect similar traffic when it is sent over IPv6.

Best practices to prevent unwanted and unauthorized IPv6 traffic from the Internet are:

- To prevent intranet hosts from using any IPv6-over-IPv4 tunneled traffic to reach the Internet, configure IPv4-based edge firewall to drop all outbound IPv4 protocol 41 packets. To prevent Internet hosts from using any IPv6-over-IPv4 tunneled traffic to reach intranet hosts, configure IPv4-based edge firewall to drop all inbound IPv4 protocol 41 packets.
- Upgrade edge firewall, proxy, and IDS to include IPv6 and tunneled IPv6 functionality.

- If private network computers must communicate with hosts on the IPv6 portion of the Internet, upgrade edge firewalls between private network and the IPv6 portion of the Internet to support stateful IPv6 firewall functionality.
- Deploy ISATAP correctly on private networks so that default route traffic is never forwarded to the IPv4 Internet. Default route traffic from ISATAP hosts on the IPv4 portion of network should be forwarded to an ISATAP router, which is connected to both the IPv4 and IPv6 portions of private network. The default route on the ISATAP router should point to the IPv6-capable portion of private network.
- If the ISATAP router and edge firewall is the same device, ensure that the device's default route for IPv6 traffic points to the IPv6 portion of your network, not to the IPv4 Internet.
- If the ISATAP router and edge firewall are different devices, configure IPv4-based edge firewall to silently discard all IPv4 traffic with the IP Protocol field set to 41 on the interface attached to the private network. This will prevent IPv4 Internet connectivity to ISATAP hosts on the private network.
- If the ISATAP hosts on private networks must communicate with hosts on the IPv6 portion of the Internet, upgrade edge firewalls between private networks and the IPv6 portion of the Internet to support stateful IPv6 firewall functionality.
- To prevent private network hosts from using Teredo traffic to reach locations on the Internet, configure IPv4-based edge firewall to silently discard all IPv4 traffic with the source or destination UDP port of 3544 on the interface attached to the private network. This will prevent Internet connectivity to Teredo hosts on the private network.

When deploying IPv6 on a network, the following security issues should be considered:

- Authorization for automatically assigned addresses and configurations.
- Protection of IP packets.
- Host protection from scanning and attacks.
- Control of what traffic is exchanged with the Internet.

In many cases, these security considerations also exist for IPv4 traffic. For most of these security considerations, there are mitigation technologies or best practices to minimize the potential risks of IPv6 traffic in current and future versions of operating system (Microsoft, 2006).

This chapter focused on the key features of IPv6 and demonstrated the similarities and differences involved with this new technology. The methods currently available in which the IPv6 transition may coexist with IPv4 have also been discussed. Issues concerning IP security and the possible hazards that can exist if functions such as auto-configuration are turned on by administrators are also covered. Now that the basics of IPv6 features have been covered, the next chapter will recommend how the current course curriculum at NPS should be modified to help students understand the IPv6 technology on a basic level and make them aware of implementation methods and issues associated with the technology transition.

### **III. EDUCATION IMPLEMENTATION INTO NAVAL POSTGRADUATE SCHOOL CURRICULUM**

#### **A. OFFICE OF MANAGEMENT AND BUDGET TIMELINE REQUIREMENT**

The purpose of this chapter is to identify what is currently taught at the Naval Postgraduate School concerning IPv6 and to recommend future course implementation. The timeline for introducing the information needs to compliment the timeline set forth by the Office of Management and Budget (OMB) for the DoD and other federal agencies' transition to IPv6. This will provide a timeline in which students are introduced to information that will be useful and pertinent by the time a graduate enters an occupation or billet that requires the application of this newly acquired knowledge.

##### **1. Initial Directives**

Initial government wide efforts to start investigating IPv6 occurred in 2003 after the President of the United States issued the *National Strategy to Secure Cyberspace*. This document identified the need for a more robust and secure mechanism for the Internet because of the nation's heavy reliance on cyberspace for day-to-day transactions. For this reason, the Department of Commerce formed a task force consisting of parties from both the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration to investigate the feasibility of using IPv6 and the implications of making the transition to this new Internet Protocol. From this research, the Department of Commerce issued a draft report in July 2004 titled *Technical and Economic Assessment of Internet Protocol Version 6*. Based on the information collected from this research and the information provided under the direction of OMB, the GAO (Government Accountability Office) issued its report in May 2005 titled *Internet Protocol version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks*. This document was vague in providing an exact timeline for the transition to occur. Instead, it gave a brief overview of IPv6 and provided tasks that needed to be accomplished for a successful transition. Additionally, it made clear that the transition was already occurring and ongoing (GAO, 2005).

On June 29, 2005, Karen Evans, Administrator for Electronic Government and Information Technology, OMB, announced a policy that established June 2008 as the deadline for all agencies' infrastructure (network backbones) to be using IPv6 and that those agencies' networks must interface with the network backbones. Once the infrastructure was in place, the applications and other elements would follow.

## **2. OMB Timeline Guideline Memorandum M-05-22**

On August 2, 2005, a memorandum from the OMB office was released. This memorandum outlined in more detail the timeline and goals required for government agencies to make the IPv6 transition.

### ***a. November 15, 2005***

- Agencies were to assign an official to lead and coordinate the agency planning.
- Report initial inventory of existing equipment that includes items such as switches, routers and firewalls
- Second inventory of missed equipment that are IPv6 compliant.
- Start an impact analysis that focuses on costs, risk mitigation, and operational impacts.

### ***b. February 2006***

- Provide progress report on inventory and impact analysis.
- Provide information required by Enterprise Architecture (EA). This information can be referenced in the attachments to the memorandum and are not necessary for the purpose of this thesis.

### ***c. June 30, 2006***

- Completed inventory submitted to OMB of second inventory.
- Completed impact analysis of operational and fiscal impacts, and risks submitted to OMB.

### ***d. June 30, 2008***

- All agencies will have IPv6 network backbone in place and agency networks must be interfaced with this infrastructure. Reports will be submitted regularly to inform OMB of each agency's progress to the deadline date.

The figure below gives a general overview of the timeline established by OMB. Although deadlines and milestones have given a goal for agencies to accomplish certain tasks, it is very likely, based on a majority of previous government projects, that the

deadlines may change. This speculation is based on the analysis that this involves a huge financial burden in a time of tight budgets. Additionally, the technology for making such a big technological change is still being developed and tested. The commercial industry as a whole has not quite accepted IPv6 as a required improvement. The push for this technology in the United States comes from the government, with the DoD taking the lead. Normally, the government follows the lead of the commercial industry, which enables commercial-off-the-shelf technology (COTS), leveraging the private industries' expense for the research and development.

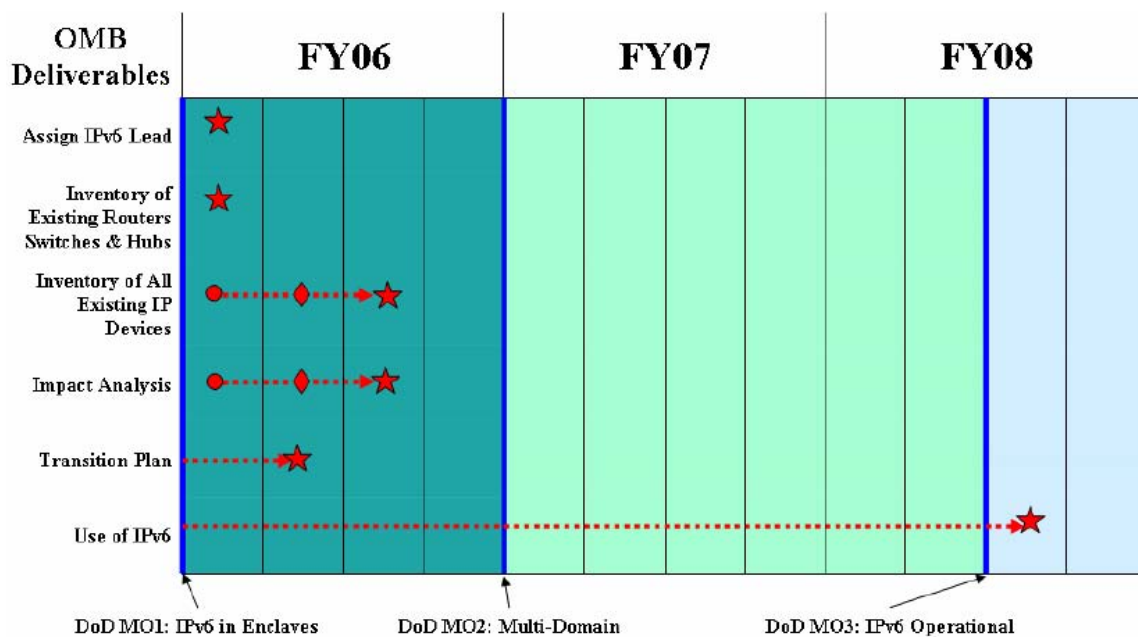


Figure 5. IPv6 Deadlines Established by OMB (Geesey, 2006).

The DoD has determined its business case and is leading the way for the IPv6 transition. The DoD has developed draft engineering plans, risk management documentation, work products, requirements criteria, budget requirements, and a master schedule (GAO). Below is a figure showing the schedule the DoD has planned for the required efforts to make the transition.

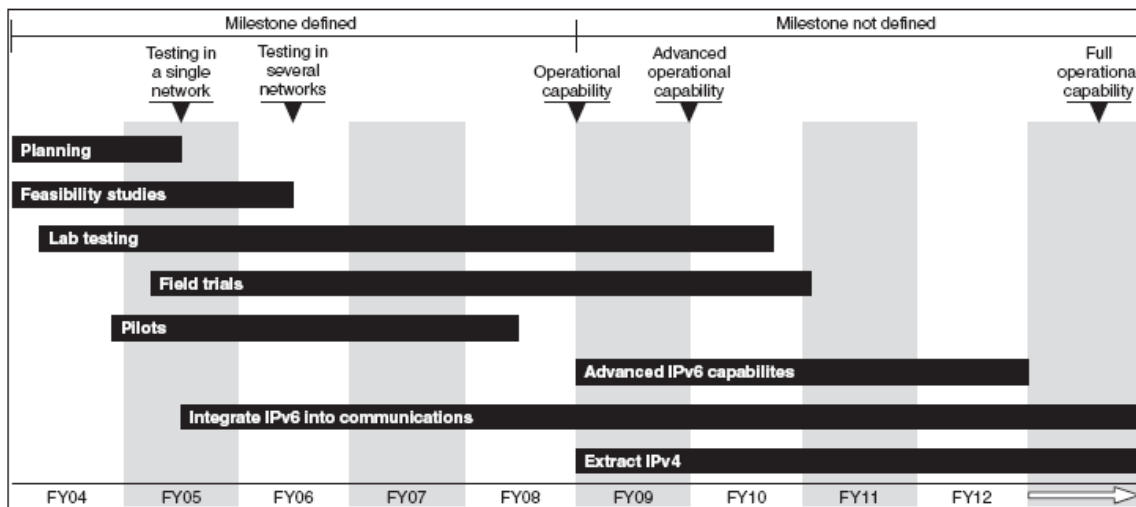


Figure 6. DoD's Schedule for IPv6 Transition (GAO, 2005)

## B. RECOMMENDED IPV6 INCLUSION FOR SELECTED COURSES AT THE NAVAL POSTGRADUATE SCHOOL

It is important that graduates of NPS headed to new jobs and billets be aware of the ongoing transition to IPv6. Although the change will be transparent to most military members, it should be understood that the implications of this transition affects military personnel and federal employees across a broad spectrum of jobs, not limited to just network administrators and developers but also financial experts, logisticians, and operational analysis experts. Most of the pertinent knowledge acquired by these military and federal employee professionals will be gained once they report to their next duty station or assigned jobs and receive the training there.. It is the intent of this thesis, however, to underscore the need for students to gain a basic understanding of IPv6 by introducing this material into the NPS curricula as soon as possible. The goal is to survey specific technology courses offered at the Naval Postgraduate School and identify what is currently taught concerning IPv6, then outline material that should be introduced into the curriculum to ensure the men and women reporting to the affected information technology billets are prepared to take on the responsibilities with which they may be challenged in future years.

Listed below are current courses offered at NPS, along with the relevant course description for each course. Every course description is directly taken from the NPS Python Course Catalogue system. These are courses that would benefit most from

changes in the curriculum to address the IPv6 transition. Recommendations for curriculum changes and additions follow each description.

### **1. Course IS3502 – Fundamentals of Networks: LAN/WAN**

The course is targeted to the analysis and design of computer and telecommunication networks in close relationship with the emerging environment of Global Information Grid (GIG). The fundamental concepts of Internet and LAN/WAN building blocks for wired, satellite, and mobile wireless communication segments of Global Information Grid are in the kernel of the course. Four-step network design decision framework is in the center of the classroom, seminar and project teamwork. This is complemented by analysis of emerging trends in high-speed terrestrial, wireless, and satellite communications. The study includes two research projects. The objective for both projects is to allow students to get hands-on experience with the analysis and design of emerging information networks. The Midterm Project is targeted to the "bottom-up" study of emerging networking technologies and their implementation within the Global Information Grid to enable command and control and sensor-decision maker networking operations. The Final Project is focused on the "top-down" design of business proposal for selected GIG networking segments enabling Command and Control, Humanitarian, ISR, UAV, METOC, and other operations. Both projects are tight to the NPS research activities with SOCOM, DHS, ONR, Foundry Networks, and Internet 2 community. The course combines on-line study with modeling exercises in OPNET IT Guru simulation modeling system. The on-line environment is comprised of the Blackboard System, interactive Agent-Evaluator for homework exercises and tests, and optional Groove client for student's collaboration with professor.

IS3502 currently covers the basics of IPv6 in Chapter 22 of Douglas Comer's book, *Computer Networks and Internets With Internet Application*. Specifics covered are a brief overview for changing to a new IP version, header format, and IPv6 addressing. These topics will suffice for a period of 9 months to a year. Because only a couple of days, if any at all, are devoted to this topic out of a 12 week course, it is necessary to investigate a new source for academic information. Joseph Davies' *Understanding IPv6* provides an academic approach to learning the new IP. The book provides a CD-Rom with prepared course material on Microsoft PowerPoint slides, and he highly encourages educators to use these slides or to supplement educator's own presentation materials with the information provided on these slides. In the timeframe of June 2007, educators will need to find a new book that covers networking technology and concepts which focus

more on specific IPv6 standards and concepts while lightly touching on IPv4 topics. This timeframe is important because this is the target group of students that will be entering new jobs and billets requiring the IPv6 knowledge. In the two to three year timeframe, this course should be predominately focused on networking topics that contain technologies incorporating IPv6. It should be noted that the course does not specifically target the Internet Protocol but networking in general. For this reason, the Davies book is not a pure solution for this course.

## **2. Course IS4188 – Collaborative Technologies**

Collaborative technologies and multiple agent decision support architectures become the central application elements of emerging Global Information Grid, FORCEnet, DARPA NICCI and other sensor-decision maker networking initiatives. The first part of the course is based on the analysis of collaboration in different human organizations and the requirements to agent-based decision support architecture. The second part of the course is focused on studies of intelligent agents and multiple agent architecture. From the beginning of the course students are involved in the hands-on practice with wireless collaborative environments including GPS units, pocket PCs, laptops, and other devices. We start with using peer-to-peer Groove collaborative tool and NPS agents-facilitators. We later move on to several demonstrations including client-server GENOA system implementation for Homeland Security and PACOM POST virtual meetings via the Lotus Same Place System.

IS4188 does not cover any topics concerning IPv6 at the time of this thesis. The description does not dive into the specifics of IP but does mention the use of communicating devices that at some point in the future may have IPv6 addresses. Additionally, the mention of the GIG implies that the integration of IPv6 will be involved in some manner. Discussions in this course should start as soon as possible. The topic of devices containing their own IP address should be discussed as a possibility and incorporated into the curriculum for this course in the June 2007 timeframe. Further research should be explored by students in how this new technology can affect the collaboration of the devices mentioned in the course description.

## **3. Course IS4505 – Wireless Networking**

This course provides students with wireless networking fundamentals essential to design, install administer and support IEEE 802.11 compliant wireless networks. The course content and format is aligned with the Planet3 Wireless Certified Wireless Network Administrator (CWNA)

Official Study Guide. Students who successfully complete this course will be prepared to take the CWNA certification exam.

Currently, IPv6 is not discussed in this course. The biggest benefit of IPv6's mobile characteristic is that even as a mobile node changes location and address, the communication the node is using remains connected and maintained. Mobile capability is one of the highlights of IPv6 and the big attraction for the DoD because of its global activities and need for mobile connection around the world and within the GIG. In the next year or two, the course will need to be restructured to address the changes required for this course. Once again, the best source for educators to exploit is Chapter 12 of Joseph Davies' book. It can be expected that the certification opportunity provided by this course will eventually change and new certification will be available. An immediate introduction to the upcoming changes created by IPv6 need to be briefly mentioned to students in the next 6 months until the full affects of the IPv6 transition on the mobile users is in full effect, around the June 2008 timeframe. At that point, the course should cover IPv6 mobile capabilities more thoroughly.

#### **4. Course IS4926 – Telecommunications and Network Operating Centers**

The course provides analytical background for implementing telecommunications management systems and integrating management infrastructure into the information grid design. It targets operations support for Global Information Grid, terrestrial, satellite, and mobile wireless network operation centers. The course combines classroom activities with research and design experience in telecommunication networks configuration, fault, and performance management. In the center of analytical work is the project based study of management functions and information models for SNMP MIBs, TMN and architectures. The advanced study issues include introduction to knowledge based management and, intelligent agents technology. The applications target the needs of Global Information Grid Operations, C4ISR networks management, Joint Experimentation, Fusion Centers, Network Operation Centers environment. They employ features of LAN/WAN networks, ATM networks, PCS networks, satellite/wireless networks, UAV, HALO, and other platforms. During the course work students will gain basic knowledge of several commercial telecommunications management systems used by the NOCs: Spectrum, HP Open View, Tivoli, Unicenter TNG, Micro Muse, etc.. The classroom studies and projects teamwork are facilitated by the on-line distributed learning and shared electronic workspace environment.

IPv6 is briefly mentioned in this course. All aspects of this course will be impacted by the implementation of IPv6. The GIG focuses on all aspects of communications and networking. An overview of IPv6 and its role in the GIG should commence as soon as feasible but no later than June 2007. IPv6 will be foundational for all topics discussed in the description. The importance of commercial telecommunications will also have a huge impact on the information taught in this course as the commercial sector within the United States is slow to accept this upcoming transition.

#### **5. Course CS3502 – Computer Communications and Networks**

This course covers basic computer networking concepts and technology through the study of protocols at each layer of the Internet architecture. Materials taught in class are reinforced through laboratory projects. Prerequisite: a solid background in Computer Architecture, Algorithm and Data Structures, and programming experience with C/C++ or Java are important for success in this class.

Much like IS3502, the basics of IPv6 address spacing and address header definitions are generically covered in this course. Within the next two years, more emphasis will have to be placed on the specifics of IPv6 and its role in networking while the information concerning IPv4 is slowly migrated out of the curriculum. A good start for introducing more topics concerning IPv6 can easily be implemented using Joseph Davies' book and complimentary PowerPoint slides contained on the CD-Rom.

#### **6. CS3505 – The Internet and the Information Highway**

In this class, the Internet and related technologies are explored. Major objectives are (1) to learn what the Internet and the "information highways" are; (2) to learn how to use the Internet for both business, academic and personal uses; and (3) to learn what is the current and especially future direction the Internet is going. Students will gain experience in exploring the World Wide Web and in creating their own home pages using the language HTML. They will also learn how to use the "big three" Internet tools, which are FTP, E-mail, and Telnet. Some background on how these protocols developed is also presented. Lectures also discuss the origins of the Internet, and the various physical and software layers which make up the Internet. The class requires a series of laboratory assignments, through which the students become familiar with the concepts in a "hands on" way. The class is intended for all graduate students interested in learning about and using the Internet, so the only prerequisite are graduate standing.

This course is already somewhat of a history course on the Internet so much of the information presented will not change. A short, one hour introduction to the upcoming IPv6 change is most certainly warranted and could be added to this course to provide more emphasis on the evolving Internet and the reason for required change if it isn't already mentioned.

#### **7. Course CS3600 – Information Assurance: Introduction to Computer Security**

This course provides a comprehensive overview of the terminology, concepts, issues, policies, and technologies associated with the fields of Information and Software Assurance. It covers the notions of threats, vulnerabilities, risks and safeguards as they pertain to the desired information security properties of confidentiality, integrity, authenticity and availability for all information that is processed, stored, or transmitted in/by information systems. This is the entry point (prerequisite) for all other Computer Security Track courses.

Currently no references are made to IPv6 in this course. Many changes will be required for this course over the next few years. The fact that IPSec is required and built into IPv6 will affect the information provided in this course. While IPSec is tighter in IPv6, trying to migrate to IPv6 creates security issues and potential hazards for information assurance. With the different methods being proposed in order to make the transition to IPv6 successful, the issue of security will be large. Specifically, prior to June 2007, the methods of tunneling and translation to make IPv6 and IPv4 work together will have to be covered. A few graduate students at the Naval Postgraduate School are working with agencies to demonstrate the vulnerabilities created by these methods which will allow the two IP versions to co-exist until the transition to a pure IPv6 backbone is completed. Frequently, these vulnerabilities and weaknesses are readily advertised on the World Wide Web and in hacker forums before the methods are employed.

#### **8. Course CS3660 – Critical Infrastructure Protection**

This course examines the critical infrastructure of the USA. Eight sectors of the critical infrastructure are examined: Banking/Finance; Health Care/Health Affairs; Space/ISR; Power/Energy; Logistics/Postal System; Transportation; Telecommunications/Satellites; and Internet/IA. Each sector and its components is characterized in terms of its vulnerabilities, especially its interdependencies and couplings with other sectors. Finally, the course identifies potential counter measures that mitigate sector and system vulnerabilities and assesses their costs and benefits.

Eventually the eight critical infrastructures listed above will in some way be reliant on IPv6. It is unclear at this time whether IPv6 will have a direct influence on these infrastructures. It will definitely have a direct influence on administrators managing those infrastructures. By June 2007, students should be informed that the transition to IPv6 is ongoing and that the methods of tunneling and translation that are used to make the transition could pose vulnerabilities to network systems that support these sectors.

#### **9. Course CS3670 – Information Assurance: Secure Management of Systems**

This course provides students with a security manager's view of the diverse management concerns associated with administering and operating an automated information system facility with minimized risk. Students will examine both the technical and non-technical security issues associated with managing a computer facility, with emphasis on DOD systems and policies. Students have the opportunity to earn the following CNSS (formerly NSTISSI) certifications: INFOSEC Professional, System Administration in Information Systems Security, and ISSO.

The problems associated with IPv6 auto-configuration, as well as the aforementioned vulnerabilities created by tunneling and translation, should have a huge impact on the information covered by this course within the next year. The pluses of IPSec and streamlined routing capabilities should also become a part of the discussion for this course.

#### **10. Course CS3690 – Network Security**

This course covers the concepts and technologies used to achieve confidentiality, integrity, and authenticity for information processed across networks. Topics include: fundamentals of TCP/IP-based networking, core network security principles, traffic filtering types and methodology, packet-level traffic analysis, employment of cryptography, tunneling/encapsulation, Public Key Infrastructure (PKI), remote authentication protocols, and virtual private networks based upon the IPSec, L2TP, and SSL protocols.

Although still limited in depth and scope, of the courses mentioned and observed prior to and during this thesis writing, CS3690 has displayed the most comprehensive coverage of IPv6. In this course, students are required to reference RFC2460, which covers IPv6, and answer homework questions related to IPv6. These questions cover a range of IPv6 topics from address spacing to address header specifics. More importantly,

the student is forced to take a look at the RFC that addresses IPv6. The current lecturer for this course, admits that the time limitation of the course prevents full coverage of topics concerning all aspects of security being faced with the IPv6 transition, and securities issues that will be faced once the transition is complete. Since the instructor for this course is a part of an IPv6 working group at NPS, he understands that changes will be required to the course in the near future in order to address security issues that will be encountered as a part of the transition to IPv6 over the next few years.

#### **11. Course CS4138 – Mobile and Wireless Security**

The application of Mobile and Wireless devices has grown rapidly in military and commercial environments. The functionality and reliability of these devices has grown tremendously. The mobile and wireless nature of these devices raise new and important security challenges not usually present in static environments. This course will address these questions including the security functionality, protocol and assurance issues associated with this emerging technology.

Much like IS4505, the mobility perks of IPv6 will need to be introduced and discussed within the course in the next year with increasing emphasis on mobility as the GIG components continue to be introduced into the market and used by military members deployed worldwide. Chapter 12 in *Understanding IPv6* is again highly recommended for immediate or near future introduction to topics that will affect this course concerning IPv6. As the transition and GIG matures in the next few years, better sources for educational material will be required.

#### **12. Course CS4550 – Computer Networks II**

This course covers advanced and emerging topics in computer networking. Some topics taught in CS3502 will be reviewed and studied in more detail. Other course subjects may vary from instructor to instructor and they include: multimedia networking, wireless networks, multicasting, peer-to-peer networks, quality of service, network management, network architecture, and security. Prerequisite: CS3502

All topics concerning IPv6 need to be briefly covered in this course starting as soon as possible if not already mentioned. Implementation of deeper coverage concerning IPv6 topics should migrate into the curriculum over the next year and be in place by June 2007. By June 2008, a reversal of IPv6 and IPv4 topic coverage should

occur as IPv4 topics are briefly touched upon and IPv6 networking topics are heavily covered. The best book to jump start the instruction within this course is Joseph Davies' book.

### **13. Course CS4552 – Network Design & Programming**

A hands-on introduction to parallel computing. The course introduces the student to different scientific and engineering applications that can benefit from parallel computing. The performance trade-offs among different ways of parallelizing an application are discussed. With the aid of parallel programming development tools, the students design, implement, debug, and monitor parallel programs for a few of the applications discussed. Every student is required to complete a nontrivial parallel program for solving some problem pertaining to his/her academic fields of study. The course is intended for CS and non-CS majors. will be guided to evaluate an emerging networking technology through experiments performed on a real network or using a Java based network emulator called SAAM. The network protocols covered in this course include: RIP, OSPF, DNS, HTTP, DHCP, TCP, UDP, and VPN. The prerequisites are: a Java Programming course, CS-3502, and CS-4550; or equivalent (with instructor's consent).

The applications that will be required to provide a smooth transition to IPv6 in some sense need to be addressed in this course especially as it is an emerging network technology. A required change for this course is not perceived as the need to address transition topics will be addressed as they appear in the next 3 years while the system is put in place to accept the IPv6 transition.

### **14. Course CS4675 – Intrusion Detection and Response**

This is an introduction to methods of intrusion detection in computer systems and networks and the possible methods of automatic responses to those events. It will cover types of intrusion detection, inference of suspicion, implementation, and management, and will examine at least one specific product. A special focus in response management will be the use of deliberate deception in defense of systems, including the psychology and ethics of deception in general. Prerequisite: CS3600.

Intrusion detection systems will be vulnerable to the transition because the tunneling methods discussed previously for allowing migration and coexistence of both IPv4 and IPv6 at the same time permits unauthorized traffic. It is imperative that this course begins to address the issue within the next 6 months. The psychology and ethics of deception as mentioned in the description will remain the same. Students should also

be instructed on the hazards of turning on auto-configuration for IPv6 without knowing the full implications of such a move when addressing IDS. Full discussion of IPv6 and IDS should be initiated by June 2008 as IPv4 IDS related material is migrated out of the course.

#### **15. Course CS4678 – Advanced Vulnerability Assessment**

This course provides a basis for understanding the potential vulnerabilities in networked systems by applying a problem-solving approach to: 1) obtaining information about a remote network, 2) possibly exploiting or subverting systems residing on that network, 3) understanding the theory of operation of existing tools and libraries along with how to measure the effectiveness of those tools, and 4) understanding tools and techniques available for vulnerability discovery and mitigation. Labs provide practical experience with current network attack and vulnerability assessment tools as well as development of new tools. Footprinting, scanning, enumeration and escalation are addressed from the attacker's perspective. A final project that demonstrates skill and knowledge is required. Prerequisites: CS3113, CS3450 and CS3690 or consent of instructor. This course is UNCLASSIFIED FOUO, U.S. Only.

This course will evolve dramatically and quickly as hackers expose new ways to break into an IPv6 capable network. This will be especially true during the migration and coexistence of two IP versions. There is already enough information contained on the World Wide Web that instructors can start introducing material immediately and adjust the curriculum to address the early vulnerabilities already exposed as IPv6 matures and is deployed throughout government agencies. The change for this course will be fast moving as vulnerabilities of IPv6 are quickly discovered and patched in the next three years.

The list above is not exhaustive and IPv6 may become the topic for discussion in other courses at the Naval Postgraduate School

#### **C. IPV6 EDUCATION OUTSIDE NAVAL POSTGRADUATE SCHOOL.**

It is foreseen that a plan to educate military and civilian personnel on the upcoming change will be a requirement for some technical schools within the military where IPv6 has an influence on operations. At the time of this writing, the only military technical school providing a response to the IPv6 transition was the U. S. Marine Corps' Basic Communications Course taught in Quantico, VA. Donnie Pritchard, the Deputy Course Coordinator, replied via email that no IPv6 topics were covered at this time.

Attempts to locate information and contact personnel at other technical schools were not successful. Consulting firms will most likely be hired to provide initial training for specific military technical schools until the understanding of IPv6 mechanics and workings become common knowledge. Until then, the information must be grabbed from sources outside of the military institutions.

### **1. Universities**

Many universities in the United States are conducting studies and setting up IPv6 pure backbones for testing and experimentation. It will be the work of universities such as these and the Naval Postgraduate School that helps promulgate the new IPv6 technology.

Currently the University of New Hampshire Interoperability Lab (UNH-IOL) works closely with Joint Interoperability Testing Command (JITC) on a project called MOON6. MOON6 is lead by the North American IPv6 Task Force (NAv6TF) which is a subchapter of the IPv6 Forum.

The Moonv6 network is a set of native IPv6 connections between sites on the global Internet that will forward packets to other Moonv6 peering sites. Participants can have a native IPv6 connection to the Internet, and Moonv6 will permit IPv6-in-IPv4 tunnel hops for a 90 day period to test on the Moonv6 network, provided the requestor, not Moonv6 administration, defines and administers those tunnels (University of New Hampshire IOL Website).

The Moon6 project allows institutions and agencies to protocol test different equipment and use real networks in order to extend research and development efforts to create confidence in IPv6 technology. UNH-IOL's website provides many links to case studies and even provides a custom software-based test tool, called TestMonkey. This software can be used to test IPv6 state machine functionality.

This is just one example of a university that has linked up with other agencies and universities to provide a starting point for implementing IPv6. There are hundreds of other universities in the United States that are setting up and running their own IPv6 networks in a lab or in cooperation with other network service providers and universities in efforts promulgate the IPv6 technology.

## 2. Consulting Firms and Training Companies

There are several consulting firms that provide education opportunities concerning IPv6. Three of these are briefly mentioned and described below.

### a. *Native6 Incorporated*

This corporation focuses solely on the topic of IPv6. They offer classroom instruction and provide field integration services. The broad range of courses are too numerous to list but the table below gives a brief overview of some IPv6 training services provided.

Native6's IPv6 Educational Offerings		
Native6 Courses		Cisco Courses
Building IPv6 Networks	Executive Overview of IPv6	IPv6 Fundamentals (IPVSF)
Programming for IPv6	Understanding IPv6 Security	IPv6 Design & Deployment (IPVSD)
Native6 Provides Course Customization		

Table 2. Native6's Education Offerings (Native6 Website)

The cost per person to attend a two- to five-day course runs into the thousands of dollars depending on the course type, but exact figures can be gathered from the website at <http://www.native6.com>. Their website also provides links to other IPv6 resources and appears to work in partnership with Cisco in their training.

### b. *Cisco Systems*

Widely known for its routers, Cisco provides training pertaining to the IPv6 transition and use of its routers and equipment to help in the transition. Below is a snippet from Cisco Systems website describing the course and can be accessed at [http://www.cisco.com/cgi-bin/front.x/wwtraining/CELC/index.cgi?action=CourseDesc&COURSE\\_ID=2235](http://www.cisco.com/cgi-bin/front.x/wwtraining/CELC/index.cgi?action=CourseDesc&COURSE_ID=2235).

Version 2.5 of the ?Implementing IPv6 Networks? course is a 3-day instructor-led training course that provides technical training to help network engineers with the implementation, configuration, and

maintenance of IPv6 networks using Cisco devices running Cisco IOS Software release 12.2T or later. This course covers routing protocols such as RIP, integrated IS-IS, BGP4+, IPv6 deployment strategies including overlay tunnels, 6PE, and NAT-PT, and other IPv6 features supported in phase 2 of IPv6 development roadmap from Cisco.

The course outline is given in great detail at the same website address. No prices are divulged and Cisco requires registration for financial details.

Cisco also provides a series of online seminars that are free of charge. Registration and details of the online seminars can be viewed here [http://www.cisco.com/cgi-bin/sreg2/register/regdetail\\_private.pl?LANGUAGE=E&METHOD=D&TOPIC\\_CODE=4142&PRIORITY\\_CODE=134566\\_1](http://www.cisco.com/cgi-bin/sreg2/register/regdetail_private.pl?LANGUAGE=E&METHOD=D&TOPIC_CODE=4142&PRIORITY_CODE=134566_1).

The particular seminar listed above addresses IPv6 transition planning for federal agencies

*c. TONEX*

This Dallas-based company provides two- to three-day onsite training as well as public training for IPv6 topics ranging from the basic fundamentals to the planning, design, and implementation of IPv6 networks. Most courses offered are in the fifteen hundred dollar range for a single person.

Many courses are only offered in certain geographical areas and on particular dates which adds to the problem of getting training and education for personnel. Onsite training provides the best source for training but does require the resources of time, personnel, and money needed to attend a course concerning the IPv6 transition.

**3. Other Education Opportunities**

The World Wide Web and the Internet are a large source for information. Reliable and trusted information concerning the IPv6 transition can be found at many sites and forums. As an example of the information available, two major sites are discussed below that can provide trusted information for educational use and have had some impact on the development of IPv6. In turn, these sites point to other good sources for educational support. Other sources have already been mentioned in both this chapter and Chapter Two of this thesis and will not be repeated.

*a. Defense Information Systems Agency*

This is a good source for information for IPv6 and its implementation into the DoD. It does require identification verification using a Common Access Card (CAC) provided by the DoD. The site can be located via the Internet at <https://disronline.disa.mil/a/DISR/index.jsp>. DISR is the DoD IT Standards Registry.

*b. The Internet Engineering Task Force (IETF)*

The mission of the IETF is to make the Internet work better. It is an international community of network designers, developers, vendors, and engineers that have an interest in improving how the Internet works. This is where links to request for comments (RFC) can be located. It explains every aspect of the Internet to include the people and working groups that comprise the IETF. A better understanding can be acquired at the IETF education Website, located at <http://edu.ietf.org>.

**D. CHAPTER CONCLUSION**

This chapter covered the different courses, with descriptions, offered at NPS that may have an impact on the IPv6 implementation and provided a recommended change to each course listed. These recommended changes took under consideration the timeline provided by OMB, the estimated time length a student will attend NPS before reporting to a duty station, and validity of IPv6 transition to the course.

Additional focus on other education resources were examined in order to provide sources for self education or for hiring a firm to provide the training required by faculty, staff, and students at NPS. This chapter identified that a lack of information was obtained to determine whether military technical schools outside of NPS were making efforts to update training and curriculums concerning IPv6. The challenge of training network administrators and staff to help with NPS's own transition is further covered in the next chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

## **IV. THE NAVAL POSTGRADUATE SCHOOL'S PROGRESS TOWARDS IPV6 TRANSITION**

### **A. BACKGROUND**

The Naval Postgraduate School is continuously upgrading its network system in efforts to provide the best education and research environment for faculty, staff, and personnel. It is not a part of the Navy Marine Corps Intranet (NMCI) so it does not receive the funds that other organizations belonging to NMCI receive. The funding for NPS's network system is provided via institutional operating funds. These funds are acquired through a budget proposal submitted through a Navy Program Objective Memorandum (POM). The proposal submitted for 2008 to address the IPv6 transition was not approved. Alternately, NPS has asked for approximately \$3.3 million from year end funds. Of those funds, it is planned to use approximately \$2.7 million to help pay for the hardware equipment replacement and infrastructure required to meet the IPv6 transition capability requirements. As of late May 2006, there have been no answers concerning the funds.

Currently, NPS is undergoing two major changes that will eventually support its IPv6 transition and are the priority for the campus in the next six months. Both address the schools' interface to two high-speed network backbones that provide Internet access service. The first one is the wide area network provided by the Defense Research and Engineering Network (DREN) and provides the campus with its military domain or .mil address. This is an OC-3 feed that has been in place and used for approximately the past 10 years. The second backbone feeding into NPS is the California Research and Education Network Digital California (CalREN DC) and provides the education domain that NPS is currently migrating towards. CalREN belongs to the Corporation for Education Networking in California (CENIC). Eventually, NPS will be connected to the CalREN High Performance Research Network (HPR). The CalREN HPR connection will provide a one gigabit pipeline into NPS that will eventually be upgraded to a 10-gigabit pipeline.

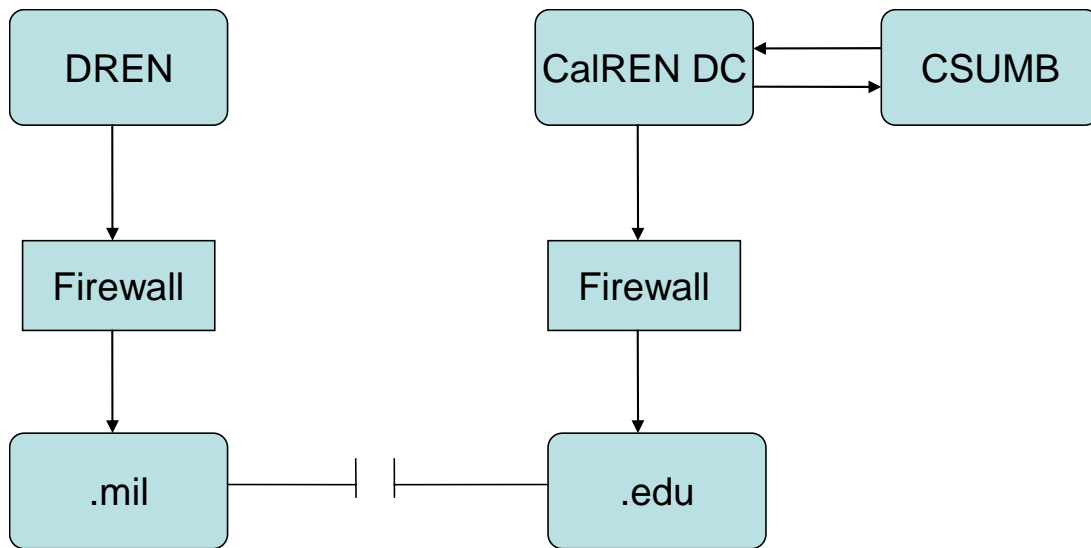


Figure 7. Basic Diagram of NPS's Current Network Infrastructure

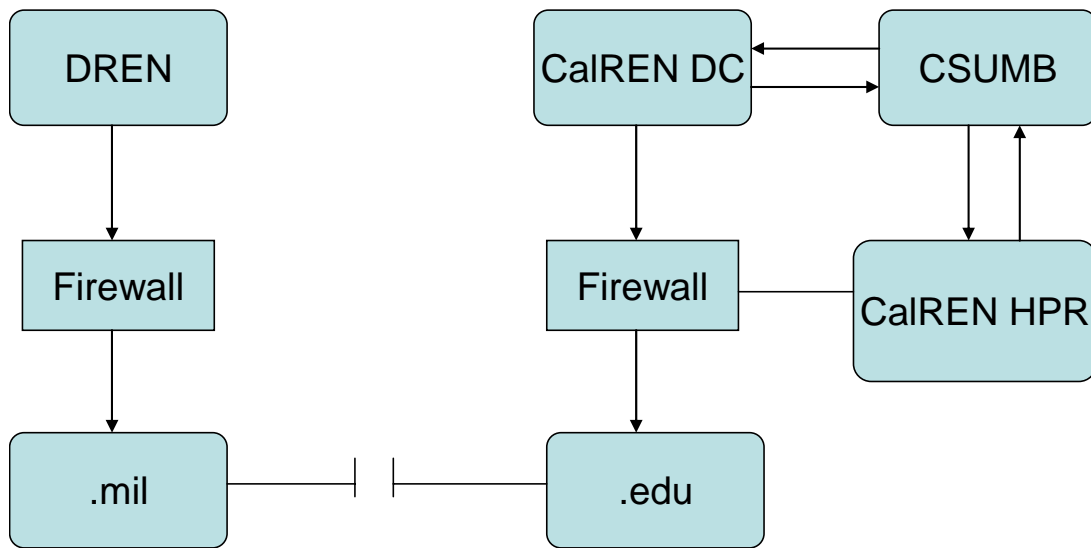


Figure 8. Basic Diagram of NPS's Future Network Infrastructure with CalNET HPR Connection

These changes are significant for NPS because eventually the CalREN HPR and DREN will become IPv6 capable. This means once NPS has upgraded its network to IPv6 capable devices, there will be a pure IPv6 backbone into NPS. NPS must also ensure its internal network is positioned to take advantage of the high speed external network to which it is gaining access.

## **B. PROGRESS TO DATE**

### **1. Monterey Peninsula IPv6 Working Group Consortium**

A working group has been established for DoD and federal agencies on the Monterey Peninsula area in efforts to share ideas and information concerning the IPv6 transition. General discussions of progress and challenges are presented at these meetings, which are currently held quarterly and sponsored by the Naval Research Laboratory (NRL) at the Navy Annex in Monterey, California. Dr. Joseph Cotham, the Assistant Information and Technology Manager, is the predominant facilitator for this working group. The main attendees of this working group are representatives from the Defense Language Institute (DLI), Defense Manpower Data Center (DMDC), Defense Personnel Security Research Center (PERSEREC), and Naval Postgraduate School. William Hogan, the Collaborative Networking Initiatives Program Manager, is the primary representative for NPS in this working group.

The NRL is a pilot site for IPv6 testing and has received IPv6 addresses for experimentation. They have participated in several exercises to include MOON6, mentioned in Chapter III. This is significant for the reason that the knowledge gained through these experiments can aid other agencies to position resources to affect the transition, learning from the experiences of NRL at Monterey.

### **2. The Plan for Naval Postgraduate School**

The biggest obstacle for not implementing an IPv6 capable network immediately is a lack of funds. Once funds are identified, the foundation for providing NPS with an IPv6 capable network can start. This delay in funding is partially mitigated in that the equipment required for this change is not quite mature.

NPS networking administrators and managers are ensuring that all necessary or immediate equipment purchases and procurements incorporate IPv6 capable technology if possible. However, NPS is foregoing a possible software upgrade to current networking equipment that will allow it to become IPv6 capable. There are two predominate reasons for not taking this opportunity to implement the IPv6 software upgrade.

First, it was determined that the software upgrade will actually slow the network systems down by as much as one-third of their current performance. This is due to the software having to do the work that an IPv6 targeted hardware device would normally be able to handle. The network traffic becomes bottlenecked as the software attempts to handle the IPv6 addressing (Cermak, 2006).

Secondly, this software will use funds for the upgrade which would only be temporary. In approximately a year, the software upgraded equipment will be replaced with IPv6 capable hardware. This is not a good return on investment. Instead of wasting the funds for the software upgrade at this time, especially when there is no support for an IPv6 network outside of NPS, the funds will be put to better use once the implementation of IPv6 capable hardware and architecture is in place to support IPv6 networks.

### **C. FUTURE PLANS**

William Hogan has submitted plans for an upgrade to the next generation network for NPS. This will eventually provide a 10-gigabit pipeline throughout the campus once the CalNET HPR connection is completed. Cost estimates are approximately \$350,000 for new single mode fiber optic connections which will supplement the multimode fiber optic media currently in place but defeats the 300 meter restriction of the latter fiber optic media. The plan also incorporates IPv6 capable hardware networking equipment that will be procured in the next five year government refresh expected to occur in the October 2007 timeframe. The plan is to first replace the two core devices and then replace all the edge devices on campus. This next generation network is another step towards providing better networking capabilities to the NPS campus while also meeting the IPv6 capability requirement.

### **D. OTHER CHALLENGES AND DECISIONS**

#### **1. IPv6 Training**

In order to successfully employ the equipment and properly manage it, the network staff must be trained on the IPv6 technology. As mentioned in Chapter III, there are consulting and training firms that provide this service but at a very hefty price tag. This is another area where pulling all the resources available via the Monterey IPv6 working group could possibly offset the cost for a single agency. It has been investigated and suggested by Michael Yee, the former CIO of DMDC, that bids be placed to different

IPv6 training companies. Once a company or consulting firm is chosen, all personnel from every agency in the working group requiring the initial training would be sent to NPS where the instruction will occur. No final plans concerning this matter have been decided. Currently, only self education is employed.

## **2. Vendor Selection**

The vendor from which to purchase hardware and equipment is also being determined. Currently, NPS is approximately 90 percent Foundry based equipment with the rest being a mix of Cisco System and legacy 3COM equipment. NPS is working closely with Foundry and Cisco to determine who will provide the most up-to-date equipment for the best price. NPS has representatives from both companies that keep regular communications in efforts to win the opportunity to supply the devices required for the upcoming changes.

The lack of education is relevant for NPS in that it can lead the way by providing a means for other agencies on the Monterey Peninsula to gain the knowledge required to understand IPv6 and implement the transition. This may eventually spread to other agencies and technical schools throughout the United States if properly planned. This is a great opportunity for NPS to advertise its institutional ability to instruct such topics on IPv6 without having to rely on the private sector for consulting help concerning the IPv6 transition and education on the topic. Lessons learned from NPS's own upgrade to the next generation network and transition to IPv6 can be used as a test bed for this education advancement as well as for other thesis research work.

THIS PAGE INTENTIONALLY LEFT BLANK

## **V. RECOMMENDATIONS AND CONCLUSION**

### **A. IMPORTANCE OF IPV6 EDUCATION IN THE CURRICULUM**

Internet Protocol version 6 is looming on the horizon and being mandated by the Department of Management and Budget for a deadline that states IPv6 capable systems must be in place by June 2008 for all government and military agencies. Currently the DoD leads the United States in moving forward with the transition. The IPv6 technology will bring many new enhancements to the Internet for the U.S., but will take time and money to complete the implementation required. One discussion among members of the Computer Science Department IPv6 working group at NPS suggested a possible analogy that the IPv6 transition may be much like the metric system implementation for the United States. An attempt to implement the standard occurred but the system was not fully embraced. It is inevitable that the transition will occur even if it is only within the DoD and government. A lack of interest from the private sector will hurt progress concerning this transition.

Regardless of whether IPv6 is accepted by the private sector, the students from the Naval Postgraduate School must be prepared to understand this change and technology as they possibly accept information and technology jobs at their next duty assignment upon graduation from NPS. This may require application of the expert skills learned on the topic of IPv6 networking. It is necessary for the faculty and staff at NPS to look to the future of this new technology and find a way to gain the knowledge required to pass this information down to students. This information is gained from online resources, through available books mentioned in this thesis, from IPv6 working groups, self teachings, or via consultants that are already subject experts on the technology. Regardless, the change to education curriculums should occur immediately, even if only the basics of IPv6 are covered in the early stages of this academic change. Naturally, over time, and as the IPv6 technology matures, the curriculum will be required to follow a steady state of change for each course. If an introduction to IPv6 occurs in the classroom within the next six months, students arriving at NPS during the 2006 to

2007 school year timeframe will hold the knowledge required to understand the IPv6 technology and be effective in applying knowledge towards the mandated DoD transition plan for year 2008.

The most important recommendation to make is for NPS to create a short 30-hour course of its own that covers all aspects of IPv6. This course would be aimed at training faculty, students desiring a more in-depth look at IPv6, and other military or DOD personnel requiring IPv6 training in order to perform required duties in the workplace. A shorter course will allow those personnel with other commitments to jobs, to learn as much as possible in the shortest amount of time. This course can be shared by the Department of Information Technology and Department of Computer Science much like IS3502 and CS3502 share the same ideas and concepts. The difficulty in establishing this idea is finding the qualified instructor that has the knowledge, credentials, and qualifications to teach such a course. If this course was well established, it might become the core center for all IPv6 training for the DoD and other government agencies.

## **B. THE BIGGEST CHALLENGES TO LEARNING**

The biggest barrier that NPS will encounter while introducing IPv6 into the curriculum and attempting to upgrade the school's own network system is money. Much of what has been researched and identified in some fashion relies on the fact that most changes require some sort of financial support or budget. The DoD has mandated this change occur, but when the hands were raised and the funds requested, the DoD denied additional funds. The funds were to be taken from an already depleted or reduced agency budget. This is a particularly difficult issue with NPS since they are not a part NMCI. Although the DoD has gone to great strides to ensure agencies do not purchase new equipment that is not IPv6 capable, it has not given much guidelines on how agencies are to achieve the 2008 timeline on limited budgets. This limited budget puts a strain on what resources NPS can use to educate teaching staff and network administrators. Research within NPS will be the biggest source of academic assistance and money for educating the staff and personnel at NPS.

The private sector's lack of interest in the new IP version also adds to the resistance for change and makes pushing this technology an even more difficult task. Fortunately, other education institutions outside of NPS are also aware of the upcoming

change and are making great strides to mature the technology and share the information. Because NPS has a close working relationship with many of these institutions, especially in California, it allows for a better learning advantage in the Monterey area.

### **C. FURTHER RESEARCH TOPICS**

Further research in the topic of IPv6 will provide numerous opportunities over the next few months to a year, and should not be confined just to the Departments of Computer and Information Sciences at NPS. As mentioned, the IPv6 implementation carries a large price tag and is the perfect focus for thesis research by finance students on the financial burdens that will be encountered by this change and possibly suggest a plan to mitigate these budget shortages. Along the same lines of this topic is whether the return on investment is advantageous for the government or even NPS itself. Finding a better Internet Protocol is important; however, the government is attempting to keep up with other countries that have turned to this technology in order to reduce the threat to the United States in the future.

Operational research students can focus on the operational impacts and management risks that will be associated with this transition. OMB has placed an emphasis on ensuring that agencies take a close look at these two topics in order to mitigate problems that might occur during the transition.

Dr. Christine Cermak, NPS Chief Information Officer, agrees that several students may find thesis topic possibilities while helping NPS with its own transition to IPv6 in the next few years. In the future, the thesis can be expanded to cover more issues that develop as NPS encounters obstacles to the transition and moves towards the next generation network currently being planned by William Hogan.

Professor Thomas Housel, Department of Information Science at NPS, is heavily involved in the process of knowledge value added (KVA). The move to IPv6 leaves the opportunity for a student to study the knowledge value added by this technology advancement and how it will affect the future of the DoD and government agencies.

The Department of Computer Science at NPS currently hosts an IPv6 working group consisting of students and faculty that are researching several different topics concerning the transition. These topics range from using covert channels to send

message traffic to analyzing the management perspective of the IPv6 transition. The topic research work done by this group can lead to revenue from government agencies, such as the Joint Interoperability Test Command in Fort Huachuca, Arizona, which seek the professional help of students and educators at NPS while forwarding the advancement of this technology.

This transition is a great opportunity for the Naval Postgraduate School to provide unique educational opportunities that support the transition to IPv6 for other agencies. This may lead to deeper research that provides funds to NPS while placing the institution on a pedestal of educational excellence. This notoriety is crucial for justifying the continuing existence of NPS, and the research and educational opportunities provided by the implementation could help with NPS's continued high standard of learning.

## BIBLIOGRAPHY

- Arkko, J., Aura, T., Kempf, J., Mantyla, V., Nikander, P., and Roe, M. (2002). *Securing IPv6 Neighbor and Router Discovery*. Retrieved May 17, 2006, from <http://research.microsoft.com/users/tuomaura/Publications/arkko+-wise02.pdf>.
- Bailey, Bliss and Carlisle, H. *IPv6 Project*. Retrieved May 22, 2006, from <https://fp.auburn.edu/internet2/ipv6.asp>.
- Brutzman, Terri. (personal communication, May 24, 2006)
- Cermak, Christina. (personal communication, May 25, 2006)
- Cisco Systems. *Cisco Seminar Series*. Retrieved April 14, 2006 from [http://www.cisco.com/cgi-bin/sreg2/register/regdetail\\_private.pl?LANGUAGE=E&METHOD=D&TOPIC\\_CODE=4142&PRIORITY\\_CODE=134566\\_1](http://www.cisco.com/cgi-bin/sreg2/register/regdetail_private.pl?LANGUAGE=E&METHOD=D&TOPIC_CODE=4142&PRIORITY_CODE=134566_1)
- Comer, Douglas. (2004). *Computer and Networks Internets With Internet Applications*. Fourth Edition. Upper Saddle River, New Jersey: Prentice Hall.
- Davies, Joseph. (2003). *Understanding IPv6*. Microsoft Press: Redmond, Washington.
- Evans, Mark. (2005). *The Navy's Transition to IPv6*. CHIPS. Fall 2004. Retrieved April 2006.
- Fulp, J. D. (personal communication, May 18, 2006)
- Geesey, Dale. (2006). *IPv6 Best Practices World Report Series: Guide for federal agencies transitioning to IPv6*. IPv6 Summit, Inc and Juniper Networks, 2005.
- Green, David, and Grillo, Bob. (2005). *The State of IPv6: a department of Defense Prospective February 2005*. SRI International. Retrieved December 12, 2005.
- Guardini, Ivano. (2006). *Migrating from IPv4 to IPv6: Planning an Effective IPv6 Transition*. Global IP Summit 2000. Retrieved May 17, 2006.
- Harrison, R., Schlabach, J., Millane, D., and Smith, S. (2005). *JITC Supports Advanced Joint Internet Protocol Interoperability Testing and Transformation Initiatives*. Received from author October 2005.
- Hogan, William. (personal communication, May 22, 2006)

- Mark, Roy. (2003). *IPv6 Transition Crucial to Military*. Retrieved May 17, 2006, from <http://www.internetnews.com/dev-news/article.php/3287191>.
- Microsoft Corporation. (2006). *IPv6 Security Considerations and Recommendations*. Retrieved May 15, 2006, from <http://www.microsoft.com/technet/itsolutions/network/ipv6/ipv6sec.mspx>.
- North American IPv6 Task Force. Retrieved May 22, 2006 from <http://www.nav6tf.org>
- Pritchard, Donnie. (personal communication, April 18, 2006)
- Sherwin, Lonna. (personal communication, June 1, 2006)
- Tonex Company. Telecom, Wireless, IT and Business Training. Retrieved May 22, 2006, from <http://www.tonex.com/>
- United States Government Accountability Office. (2005). *Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks*. Retrieved December 10, 2005, from <http://www.gao.gov/new.items/d05845t.pdf>.
- United States Office of Management and Budget. (2005). *Statement of the Honorable Karen Evans administrator for Electronic Government and Information Technology Office of Management and Budget Before the Committee on Government Reform US House Of Representative*. Retrieved May 19, 2006, from <http://www.whitehouse.gov/omb/legislative/testimony/evans/evans052905.html>.
- University of New Hampshire. *Moon6*. Retrieved May 22, 2006, from <http://moonv6.iol.unh.edu>

## **INITIAL DISTRIBUTION LIST**

1. Defense Technical Information Center  
Fort Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Marine Corps Representative  
Naval Postgraduate School  
Monterey, California
4. Director, Training and Education, MCCDC, Code C46  
Quantico, Virginia
5. Director, Marine Corps Research Center, MCCDC, Code C40RC  
Quantico, Virginia
6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)  
Camp Pendleton, California
7. Geoffrey Xie  
Naval Postgraduate School  
Monterey, California
8. John Gibson  
Naval Postgraduate School  
Monterey, California
9. Kristen Tsolis  
Naval Postgraduate School  
Monterey, California
10. Dan Boger  
Naval Postgraduate School  
Monterey, California
11. James Kay  
Naval Postgraduate School  
Monterey, California